

IN THE UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF OHIO  
EASTERN DIVISION

|                           |   |                         |
|---------------------------|---|-------------------------|
| UNITED STATES OF AMERICA, | ) | CASE NO. 1:15-CR-275    |
|                           | ) |                         |
| Plaintiff,                | ) | JUDGE DAN AARON POLSTER |
|                           | ) |                         |
| v.                        | ) |                         |
|                           | ) | <u>MOTION TO COMPEL</u> |
| JOHN CLEMENTS,            | ) | <u>DISCOVERY</u>        |
|                           | ) |                         |
| Defendant.                | ) |                         |
|                           | ) |                         |

Now comes Defendant, John Clements, by and through undersigned counsel, and hereby respectfully requests that this Honorable Court issue an Order directing the Government to produce previously requested information regarding Shareaza LE, which is the computer software program utilized by the Government during the course of its investigation of Mr. Clements. Defendant so moves pursuant to Rule 16 of the Federal Rules of Criminal Procedure as well as *Brady v. Maryland*, 373 U.S. 83 (1963) and *Giglio v. United States*, 405 U.S. 150 (1972). The items requested constitute documents or data that is material to preparing a defense against the Government's case-in-chief at trial. This Motion is based on the Fifth, Sixth and Fourteenth Amendments to the United States Constitution and Rule 16(a)(1) of the Federal Rules of Criminal Procedure. Reasons in support of the instant request are set forth more fully in the Memorandum in Support, which is attached hereto and incorporated herein by express reference.

Respectfully submitted,

/s/ Eric C. Nemecek

IAN N. FRIEDMAN (0068630)

ERIC C. NEMECEK (0083195)

Counsel for Defendant

Friedman & Nemecek, L.L.C.

1360 E. 9<sup>th</sup> Street, Suite 650

Cleveland, OH 44114

Phone: (216) 928-7700

Email: inf@fanlegal.com

ecn@fanlegal.com

**CERTIFICATE OF SERVICE**

A copy of the foregoing Motion has been served electronically this 18<sup>th</sup> day of January, 2016, to Brian McDonough, Assistant United States Attorney, United States Courthouse, Northern District of Ohio, 801 Superior Avenue W., Suite 400, Cleveland, Ohio 44113.

/s/ Eric C. Nemecek

IAN N. FRIEDMAN

ERIC C. NEMECEK

Counsel for Defendant

## MEMORANDUM IN SUPPORT

### I. Facts and Procedural History

Defendant, John Clements, is charged with one count of receiving and distributing child pornography in violation of 18 U.S.C. § 2252(a)(2)<sup>1</sup> and one count of possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). The Government's initial discovery response referenced a specialized computer software program, Shareaza LE, that was utilized by law enforcement agents during their investigation in this case. According to the discovery materials, Detective Don Seamon utilized Shareaza LE, in conjunction with Grid Cop (CPS) website, to search for Internet Protocol ("IP") addresses of network users who have recently been identified as having files of child pornography available for download.

In his report, Detective Seamon notes that the CPS database identified a particular IP address as having 395 Child Notable files. The report further states that this IP address has been directly browsed on two (2) occasions between February 25, 2014 and May 5, 2015. Detective Seamon asserts that on May 5, 2014, he was able to successfully complete four single source download files of suspected child pornography and several incomplete files from this IP address.

On May 17, 2014, Detective Seamon utilized the American Registry for Internet Numbers (ARIN) and determined that the aforementioned IP address was registered to AT&T Services. That same date, Detective Seamon requested that the Lake County Prosecutor's Office issue a Subpoena to AT&T Services to obtain subscriber information for this IP address. The response to said Subpoena indicated that Clements was the user

---

<sup>1</sup> Count 1, which alleges that Clements received and distributed child pornography,

assigned to that IP address. The information generated from Shareaza LE, CPS and the Subpoena was utilized by Detective Seamon in order to obtain a search warrant for Clements' residence.

On June 2, 2014, Detective Seamon prepared an Affidavit in support of his request for a search warrant of Clements' residence. A copy of Detective Seamon's Affidavit in support of the search warrant is attached hereto as Exhibit "A" and is incorporated herein by express reference. The Affidavit was submitted to and approved by a Judge of the Lake County Court of Common Pleas that same day. On June 3, 2014, law enforcement officers executed the search warrant at Clements' home and seized several items, which were subsequently forensically analyzed by law enforcement agents.

As a result of the Government's investigation in this case, Clements was indicted on July 21, 2015 with the foregoing offenses. After receiving the Government's initial discovery response, defense counsel retained the services of Tami Loehrs of Loehrs & Associates, L.L.C., to conduct an independent forensic examination of the electronic evidence that was seized in connection with the search warrants. Ms. Loehrs has extensive experience conducting forensic examinations in child pornography cases and is acutely familiar with the investigative aspects of such cases, including the Government's use of specialized forensic software.

Based upon her review of the evidence as well as her prior experience with law enforcement's use of modified software programs, Ms. Loehrs opines that an independent forensic examination of the Shareaza LE software is necessary in order to determine the

---

contains a date range of February 25, 2014 through May 5, 2014.

validity and/or reliability of the Government's forensic evidence – which was a product of the Shareaza LE software – as well as to determine whether the software conducted a search of Clements' computer beyond the scope of what was publicly available.

Ms. Loehrs authored an Affidavit containing a detailed explanation of how the use of the Shareaza LE software could conceivably have conducted a search of Clements' computer – prior to the issuance of any search warrant(s) – for files that were not otherwise publicly available. A copy of Ms. Loehrs' Affidavit is attached hereto as Exhibit "B" and is incorporated herein by express reference. Specifically, Ms. Loehrs notes that "[i]n this case, there is particular concern regarding the ability of the [law enforcement] software going beyond the scope of "publicly available information." *See* Exhibit "B." In support of this contention, Ms. Loehrs explains that the discovery materials contain a Screen Shot of Clements' computer, which revealed information regarding the user's (*i.e.* Clements') potential key word searches and "key strokes." Importantly, "[t]his type of data is not publicly available information, is not known by the user, and cannot be obtained with any commercially available P2P<sup>2</sup> file sharing software." *See* Exhibit "B."

Ms. Loehrs also discusses her knowledge of and prior experience with law enforcement's use of this type of software during their investigations in similar cases. She contends that the CPO software herein at issue was developed by William Wiltse, who was formerly employed by a Florida-based company, TLO. *See* Exhibit "B." Ms. Loehrs explains that Wiltse develops software that is utilized by law enforcement agencies in their

---

<sup>2</sup> "P2P" is an acronym for Peer-to-Peer, which describes a specific software program that searches for other computer users connected to the same network to locate – and download

investigations of child exploitation crimes. Ms. Loehrs also indicates that she has been involved in numerous cases throughout the country wherein this software – or variations of the software – was at issue. *See* Exhibit “B.”

Although Wiltse was formerly employed by TLO, the undersigned has learned that this Company filed for Bankruptcy in 2013 and, at the present time, no longer appears to be operational. However, counsel has determined that Wiltse is currently employed with the Child Rescue Coalition, Inc. (hereinafter “CRC”), which is located at the same physical address/location as TLO. Furthermore, a review of the CRC’s website indicates that many – if not all – of the same individuals who were responsible for developing and implementing the CPO software are also employed at the CRC.<sup>3</sup> Regardless of which particular Company developed the Shareaza LE software, the undersigned submits that the materials herein requested are available to the Government insofar as its agents have access to – and continue to utilize – the software during the course of its investigations in these cases.

In response to Ms. Loehrs’ conclusions, *see* Exhibit “B,” defense counsel sent a letter to Assistant United States Attorney Brian McDonough on December 8, 2015, requesting that he produce discovery relating to Shareaza LE software program that was utilized by law enforcement in this case. A copy of this letter is attached hereto as Exhibit “C” and is

---

– desired content (*e.g.* files, videos, images, etc.).

<sup>3</sup> A Subpoena *duces tecum* was issued to CRC requesting the same materials and/or access as set forth in the instant request. The process server has informed the undersigned that the Subpoena was properly served on or about January 13, 2016. To date, counsel has not received any response to the Subpoena, nor has their expert been permitted access to the Shareaza LE software. about

incorporated herein by express reference. Having received no response from the Government, counsel sent a second letter to AUSA McDonough on December 14, 2015, requesting that the same material be provided forthwith. A copy of that letter is attached hereto as Exhibit "D" and is incorporated herein by express reference.

On or about December 21, 2015, the undersigned spoke with AUSA McDonough over the phone to discuss the nature of the discovery request – *i.e.* an independent forensic analysis of the Shareaza LE software. During that conversation, AUSA McDonough indicated that he would obtain some additional discovery materials from law enforcement regarding the software that had not previously been provided to the undersigned, including the file logs that were generated by the Shareaza LE software during the investigation of this case. He also stated that he would discuss counsel's request for access to the Shareaza LE software with the agents.

The Government provided the file logs to defense counsel on January 8, 2016 along with a letter. A copy of that letter is attached hereto as Exhibit "E" and is incorporated herein by express reference. Counsel again queried as to whether its expert would be permitted access to the Shareaza LE software as originally requested. On January 13, 2016, AUSA McDonough responded via email and indicated that: "[t]he Government will not be providing the Shareaza LE software to your expert in this case. Among other reasons, the software is sensitive in nature, non-public, and proprietary."

As the foregoing information establishes, counsel has made reasonable and repeated efforts to obtain the requested materials and access to the Software through the discovery

process since determining that such information was necessary for purposes of defending the charges in this case. At the present time, the Government maintains that they will not provide any additional information regarding the software, nor will they allow counsel's expert to examine the Shareaza LE software as requested. For the reasons that follow, Clements respectfully requests that this Honorable Court issue an Order compelling the Government to disclose and/or produce these items forthwith.

## **II. LAW AND ARGUMENT**

Rule 16 of the Federal Rules of Criminal Procedure states that a criminal defendant has the right to inspect all documents, data, or tangible items within the Government's "possession, custody, or control" that are "material to preparing the defense." Fed. R. Crim.P. 16(a)(1)(E). Evidence is "material" if it is "helpful" to the development of a possible defense. *See United States v. Olano*, 62 F.3d 1180, 1203 (9<sup>th</sup> Cir. 1995); *see also United States v. Dobbins*, 482 Fed. Appx. 35, 41 (6<sup>th</sup> Cir. 2012). In *Brady v. Maryland*, 373 U.S. 83, 87 (1963), the United States Supreme Court ruled that the suppression by the prosecution of evidence favorable to the accused, upon request for disclosure by the accused, violates due process. The Supreme Court further expanded an accused's right to evidence held by the Government in *Giglio v. United States*, 405 U.S. 150 (1972), to include evidence that could be used to impeach Government witnesses. Pursuant to Rule 16, *Brady* and *Giglio*, the Government is required to produce the requested information regarding Shareaza LE because it is material to the development of a defense in this case and is necessary in order to effectively cross-examine Detective Seamon at trial.



**A. Discovery of Shareaza LE is Relevant and Material to Clements' Defense**

**1. *The Shareaza LE software is a critical component of the Government's case-in-chief***

Detective Seamon used the Shareaza LE software to identify an IP address, 99.105.84.152, that was alleged to have made child pornography materials available for download to other P2P users. Detective Seamon thereafter used the specialized software to connect to Clements' computer and allegedly download videos of child pornography by use of a P2P file-sharing network. Although this "search" was conducted prior to the issuance of a warrant, the Government maintains that all files that were browsed and/or downloaded from the aforementioned IP address were "publicly available." Detective Seamon alleges that he completed four single-source download files from Clements' computer, which form the factual basis underlying the distribution offense set forth in Count 1 of the Indictment.

As the foregoing establishes, the Shareaza LE software is a critical component of the Government's case-in-chief. Detective Seamon utilized this software to identify Clements' IP address and to allegedly download files of suspected child pornography during the course of the Government's investigation. The purported downloads form the entire basis for the receipt and distribution offense set forth in Count 1 of the Indictment. To that end, the Government's ability to prove the first element of the distribution charges, that Clements "knowingly distributed" child pornography by use of his computer, is dependent upon whether the downloaded files were "publicly available." Therefore, the reliability of the software as well as its ability to properly distinguish between "publicly available" and

non-shared files is squarely at issue in this case.

Moreover, all evidence relied upon to obtain the search warrant – including the issuance of the Subpoena to AT&T Services as well as the Affidavit in support of the search warrant – was a product of the Shareaza LE software. In this regard, the evidence seized from Clements’ residence supports the Government’s additional charge of possessing child pornography. To the extent that the Shareaza LE software conducted a search of Clements’ computer beyond the scope of what would have been “publicly available,” law enforcement agents violated Clements’ Fourth Amendment rights. Assuming this is established, all evidence seized in connection with this investigation – including the evidence relating to the possession of child pornography charge set forth in Count 2 of the Indictment – would be subject to suppression. This puts directly at issue the use of Shareaza LE to obtain access to Clements’ computer.

In *United States v. Budziak*, 697 F.3d 1105 (9<sup>th</sup> Cir. 2012), the Ninth Circuit Court of Appeals overruled the district court’s refusal to Order the disclosure of discovery relating to a similar FBI-run computer program, “EP2P,” in a child pornography distribution case. *Id.* at 1107. Utilizing EP2P, two FBI agents downloaded images from an IP address registered to Budziak. *Id.* The software used by the agents was described as an enhanced version of a publicly available P2P file sharing program that allowed the FBI to view all files that a particular user on the file sharing network had made publicly available. *Id.* Based on the images downloaded using the software, the FBI obtained a search warrant, which ultimately resulted in an Indictment being issued. Budziak filed a Motion to compel

the discovery of the technical specifications of the software program as well as access to a copy of the installable software for an independent forensic review. After these requests were denied, the agents were permitted to testify concerning their investigation, including their utilization of the aforementioned software. *Id.* at 1108.

On appeal, the Ninth Circuit vacated Budziak's conviction and remanded the case back to the district court. The Ninth Circuit expressly held that Budziak had made the requisite showing that such information was material to his defense of the case: "[g]iven that the distribution charge against Budziak was premised on the FBI's use of the EP2P program to download files from him, it is logical to conclude that the functions of the program were relevant to his defense." *Id.* at 1112. The Ninth Circuit analogized the issue to K-9 drug sniff cases. The court noted that defense counsel is routinely entitled to discovery on the narcotics detector dog because evidence of the dog's qualifications are crucial to the ability to assess the dog's reliability and to conduct effective cross-examination of the dog's handler. *Id.* at 1112, citing *United States v. Cedano-Arellano*, 332 F.3d 568 (9<sup>th</sup> Cir. 2003).

In the matter *sub judice*, the Indictment and discovery materials clearly establish that the Government's theory of distribution rests exclusively on the alleged transmission of images that occurred during the undercover investigation of this case. Thus, any deficiencies in the investigative software used to identify P2P transmissions that might disprove either actual or attempted distribution of child pornography would be "material" to preparing the defense, *see* Fed. R. Crim. P. 16(a)(1)(E), and therefore subject to disclosure

by the Government. *See United States v. De Los Santos*, 810 F.2d 1326, 1330 (5<sup>th</sup> Cir. 1987)(holding that evidence is “material” when it would be helpful to the defense in preparing for trial). These deficiencies would similarly be considered exculpatory and, thus, subject to disclosure under *Brady, supra*.

**2. *Access to the Shareaza LE software is necessary to cross-examine Government witnesses***

According to the discovery materials provided to date, Detective Seamon is the lone witness who used Shareaza LE software to directly connect with Clements’ computer and download child pornography. In his search warrant Affidavit, Detective Seamon asserts that between February 25, 2014 and May 5, 2014, he conducted online P2P investigations on the Gnutella network.<sup>4</sup> Through utilization of Shareaza LE and CPS, Detective Seamon was allegedly able to connect to Clements’ computer, search for files of suspected child pornography in Clements’ “shared” (*i.e.* public) folders, and complete downloads of the purported contraband.

In order to effectively cross-examine Detective Seamon on the reliability and functionality of the Shareaza LE software, defense counsel must be provided access to the software and its technical specifications. Whether Clements knowingly shared child pornography hinges on the technical specifications and reliability of this computer software program. Furthermore, whether the software enabled law enforcement to conduct a warrantless search of Clements’ computers can only be established by permitting

---

<sup>4</sup> Per Detective Seamon’s Affidavit, “Gnutella 2 is a P2P file sharing network used to exchange files between computers. The Gnutella 2 network, like other P2P file sharing networks, uses file hashing to uniquely identify files on the network and users typically locate files with keyword searches.” *See* Exhibit “B.”

counsel and its expert access to the requested materials.

In *Budziak*, *supra*, the Ninth Circuit explained that “access to the EP2P software was crucial to Budziak’s ability to assess the program and the testimony of the FBI agents who used it to build the case against him.” *Budziak*, 697 F.3d at 1112. In this regard, it was not sufficient that the defendant had the ability to cross-examine the agent at trial because he was denied the “background material on the software that could have enabled him to pursue a more effective examination.” *Id.* Citing the Third and Second Circuits, the Ninth Circuit emphasized that “a party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately.” *Id.*, citing *United States v. Liebert*, 519 F.2d 542, 547-48 (3<sup>rd</sup> Cir. 1975) and *United States v. Dioguardi*, 428 F.2d 1033, 1038 (2<sup>nd</sup> Cir. 1970)(“[i]t is quite incomprehensible that the prosecution should tender a witness to state the results of a computer’s operations without having the program available for defense scrutiny and use on cross-examination if desired”).

**3. *Concerns regarding the validity and functionality of the software can only be resolved through independent evaluation***

In the case at bar, the defense has specifically articulated concerns regarding the operation of the Shareaza LE software and its ability (or lack thereof) to limit its search to those files that are designated as “publicly available” files. These concerns are further exacerbated by Ms. Loehrs’ forensic examination of the electronic evidence that was seized in this case. Specifically, Ms. Loehrs contends that none of the files identified by Detective

Seamon during the undercover investigation of this case were found on any of the evidentiary items seized from Clements' residence. *See* Exhibit "B." Although there are text fragments of files contained on one of the devices, there is no evidence to substantiate that any of these files were contained in the "shared" folder of the computer at the time that they were allegedly identified and downloaded by the Shareaza LE software. *See* Exhibit "B."

Concerns regarding the reliability and functionality of the software are also raised by the seemingly contradictory information provided in the discovery materials as well as Ms. Loehrs' own forensic examination of the digital evidence in this case. For instance, Detective Seamon's Affidavit references the fact that particular files were downloaded from Clements' computer on May 5, 2014. *See* Exhibit "A." However, the discovery materials provided by the Government suggest that the Shareaza LE software did not complete a download of the particular files until May 6, 2014. *See* Exhibit "B." This suggests that the particular files may not have been on Clements' computer – or publicly available – on the date that Detective Seamon is alleged to have downloaded the materials from Clements' computer. At the very least, this raises serious questions about the reliability of the Shareaza LE software sufficient to warrant an independent forensic analysis.

Clements is not obligated to merely rely upon the Government's representations concerning the reliability and/or functionality of the software or that his own separate investigation would be unfruitful. *See Budziak*, 697 at 1113. Additionally, any such representations must be evaluated in light of the fact that the Government does not own

the Shareaza LE software, nor was it in any way responsible for its development. Because the software was developed by a private citizen who maintains exclusive ownership over the software, the Government has no personal knowledge as to the reliability and/or functionality of the Shareaza LE software.

It is undisputed that Detective Seamon did not develop the Shareaza LE software. Upon information and belief, Detective Seamon does not have access to the source code and is therefore unable to authenticate the functionality of the software – that is, Detective Seamon has no personal knowledge as to whether the software limits its search to files that are made publicly available. Accordingly, neither Detective Seamon nor any other law enforcement agent involved in this case can attest to the reliability or functionality of the Shareaza LE software with any degree of certainty or personal knowledge. Rather, any determination as to the functionality or reliability of the Shareaza LE software can only be made after independent analysis and testing is conducted.

In addition to these authentication issues, the defense's forensic examination has raised serious concerns regarding the reliability and functionality of the Shareaza LE software in this case. *See Exhibit "B."* Again, the evidence generated by this software bears directly on the evidence underlying Count 1 of the Indictment – evidence that the Government intends to introduce against Clements at the trial of this matter. Because of its relevance and materiality to the case, and in light of the serious concerns heretofore discussed, counsel submits that its expert must be permitted to conduct an independent examination of the Shareaza LE software in this case. Absent an Order from this Court,

Clements' constitutional rights to due process of law as well as his right to confrontation will be irreparably infringed.

**B. Public Policy Weighs in Favor of Disclosure and Access to the Software**

It is respectfully submitted that Clements has made a sufficient showing regarding the relevance and helpfulness of the discovery materials herein at issue. This Court must therefore balance the public's interest in protecting the flow of information against the defendant's right to prepare his or her defense. *United States v. Whitney*, 633 F.2d 902, 911 (9<sup>th</sup> Cir.1980); *Roviaro v. United States*, 353 U.S. 53, 62 (1957) ("[w]hether a proper balance renders nondisclosure erroneous must depend on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, the possible significance of the [undisclosed evidence], and other relevant factors").

The only justifications offered by the Government in opposition to this request are that the software is sensitive, proprietary and non-public. While counsel recognizes the importance of these considerations, it is respectfully submitted that they must be weighed against Clements' significant constitutional interests in receiving due process of law and a fair trial, including his right to prepare an effective defense and his right to confrontation. Furthermore, it is important to note that the concerns expressed by the Government can be adequately addressed through the issuance of strict protection Orders prohibiting the disclosure or dissemination of any information obtained during the course of the independent evaluation of the software.



### III. CONCLUSION

It is respectfully submitted that the facts and circumstances of this case are identical to those at issue in *Budziak, supra*. In order to assess the reliability and functionality of the Shareaza LE software and effectively cross-examine the witness who used it to download files from Clements' computer, the defense must be permitted access to the program itself. This is especially crucial when the charges "against the defendant [are] predicated largely on computer software functioning in the manner described by the Government, and the Government is the only party with access to that software." *Budziak*, 697 F.3d at 1113. Detective Seamon's use of Shareaza LE has put the software directly at issue – that is, the fact that Clements' charges arise out of the Shareaza LE software investigation makes access to this software material to the defense of this case.

Recent decisions from other jurisdictions provide further support for the proposition that when a Government investigation involves the use of computer software to obtain a search warrant and eventual Indictment, defendants should be afforded access to the software and its specifications. *See, e.g., United States v. Todd Hartman*, 8:15-cr-00063 (U.S. D.C. CA 2015) (doc. 87)<sup>5</sup>; *United States v. John Crow*, 1:11-cr-01690 (U.S. D.C. N.M. 2013) (doc. 88)<sup>6</sup>; *United States v. Angel Ocasio*, 3:11-cr-02728 (U.S. D.C. W.D. TX 2013) (doc. 150).<sup>7</sup>

---

<sup>5</sup> The Order is attached hereto as Exhibit "F" and is incorporated herein by express reference.

<sup>6</sup> The Order is attached hereto as Exhibit "G" and is incorporated herein by express reference.

<sup>7</sup> The Order is attached hereto as Exhibit "H" and is incorporated herein by express reference.

As aforementioned, the defense has articulated specific concerns regarding the operation of the Shareaza LE software and its ability (or lack thereof) to limit its search to those files that are designated as “publicly available” files. These concerns are premised not only on Ms. Loehrs prior knowledge and experience with the Government’s use of specialized software in similar cases, but also upon her own analysis of the evidence in this case. These concerns bear directly on the strength of the Government’s evidence and the reliability and credibility of its witnesses. Furthermore, there exists the very real possibility that the Government’s use of the Shareaza LE software constituted an unlawful, warrantless search of Clements’ computer that, if established, would render all evidence seized in this case subject to suppression.

Based upon the foregoing analysis, as well as additional evidence and arguments to be presented at a hearing on this matter, the undersigned submits that they are entitled to the materials heretofore requested concerning the software that was utilized by law enforcement in connection with this case. Accordingly, Clements respectfully requests that this Honorable Court issue an Order compelling the Government to provide defense counsel with the following materials and/or items forthwith:

- An installable, working copy of the software known as “Child Protection System,” including the Shareaza LE software program used by Detective Don Seamon of the Lake County Sheriff’s Office, FBI Child Exploitation Task Force and/or ICAC Department/Division, during the investigation of this case. If different versions of this software(s) exist, please provide copies of the versions used by Seamon during his investigation of Mr. Clements.

- All documents and records in the Government's possession, custody and control – including any documents and records in the possession, custody and control of other law enforcement agencies involved with the investigation of this case, including, but not limited to, the Lake County Sheriff's Department, Federal Bureau of Investigation, and/or ICAC Department/Division – regarding the Child Protection System, including the Shareaza LE software program utilized in this case. This request includes documents concerning the software's technical specifications.
- All documents and records in the Government's possession, custody and control – including any documents and records in the possession, custody and control of other law enforcement agencies involved with the investigation of this case, including, but not limited to, the Lake County Sheriff's Department, Federal Bureau of Investigation and/or ICAC Department/Division – regarding any other software, computer programs, or the like, used by Detective Seamon throughout the course of his investigation of Mr. Clements.

**WHEREFORE**, Defendant, John Clements, hereby respectfully requests that this Honorable Court issue an Order compelling the Government to produce and provide the above-referenced materials to defense counsel.

Respectfully submitted,

/s/ Eric C. Nemecek

IAN N. FRIEDMAN (0068630)

ERIC C. NEMECEK (0083195)

Counsel for Defendant

Friedman & Nemecek, L.L.C.

1360 E. 9<sup>th</sup> Street, Suite 650

Cleveland, OH 44114

Phone: (216) 928-7700

Email: inf@fanlegal.com

ecn@fanlegal.com